Hic sunt dracones Here, There Be Dragons

The perils of modern medical practice

By Nicole Li and Matthew McCoy

> "There are only two types of companies: those that have been hacked, and those that will be."
>
> —FBI Director Robert Mueller, March 2012.[1]

Our modern world contains "dragons" that are unimaginable to the technologically challenged. It also includes familiar risks like theft and loss. Spools of fax paper, rolls of stamps, and long lines at the bank are nearly obsolete, but our professional world includes pirates, Trojan horses, and trolls. The modern physician may now have a virtual office, communicate with patients via the Internet, and keep electronic medical records (EMRs). Criminals have similarly adapted.

Cybercrimes against physicians range from literal smash-and-grab of devices to highly sophisticated online deceptions. Targets may be personal identification, banking information, or proprietary information. While EMRs may help coordinate patient care and improve documentation, they also present a new trove to be plundered by those who are criminally motivated.

Forbes magazine selected cybersecurity as the top U.S. health care story of 2014.[2] A SANS Health Care Cyberthreat Report cites an alarming 94 percent of medical institutions had been victims of some form of cyberattack.[3] As technology evolves, areas that cyber criminals can exploit increases. It may be impossible to wholly protect confidential material, according to FBI Director Robert Mueller.[4] Of the many imperceptible perils of this modern age, perhaps the most likely threat to your practice is absent-mindedness. Whether by your own or a member of your staff's inadvertent mistake, a laptop is stolen, or the wrong file is attached to an email.

HIPAA's Security Rule lays out what is required of medical practices when holding and securing data. It acknowledges the diversity of medical practices, and therefore does not mandate the same measures of every covered entity. Rather, it is a flexible and scalable framework, allowing a practice to analyze its own needs and implement solutions appropriate for its business. Variables considered are the size and capabilities of a business, its technical infrastructure, the costs of security measures, and the likelihood and possible impact of potential risk to protected health information (PHI).[5] In short, HIPAA's security rule recognizes that not all organizations have the same needs, or resources, and allows them to design their own security plans accordingly.

This is good news for small and medium-sized operations that do not have vast IT and security resources. HIPAA's Security Rule recognizes that these organizations may not have the resources to prevent a breach completely. Nonetheless, it does not wholly absolve them from liability if a breach does happen. In the event of a breach, government officials will consider what security measures were in place. Likewise, as breaches become increasingly common, it is important to plan ahead, and to plan accordingly. Certain measures, if conducted ahead of time, can reduce the risk and fallout from a breach.

Assess your risk

It is impossible to eliminate risk entirely. HIPAA's Security Rule does not demand perfection. It requires entities to evaluate the likelihood and impact of breaches to Protected Health Information (PHI) so that security measures can be implemented accordingly.[6] Large companies and large data sets may be targets for network intrusions and data breaches. For smaller entities, a stolen or lost laptop may be a more likely risk. It is important to consider

1. Cowley S, "FBI Director: Cybercrime will eclipse terrorism." CNN Money, March 12, 2012, *http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm?iid=EL*.
2. Munro D, "The Top U.S. Healthcare Story for 2014: Cybersecurity." *Forbes*, Dec. 12, 2014, *http://www.forbes.com/sites/danmunro/2014/12/21/the-top-u-s-healthcare-story-for-2014-cybersecurity/*.
3. SANS Institute, SANS Health Care Cyberthreat Report 2, Feb. 2014.
4. "FBI Director: Cybercrime will eclipse terrorism."
5. Security Standards: General Rules 45 C.F.R. § 164.306(b)(2).
6. 45 C.F.R. § 164.306(b)(iv).

FIRST PRINTED IN THE JULY/AUG 2015 "BULLETIN" VOL. 94 NO. 4 REPRINTED WITH PERMISSION OF THE KING COUNTY MEDICAL SOCIETY

the types of scenarios that could occur, along with appropriate responses.

Know whom to call

As a covered entity, you are ultimately responsible for the PHI you hold. Any "health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA"[7] must institute measures to protect patient information.

Covered entities are required to notify affected individuals when PHI has been, or is reasonably believed to have been, breached. If the breach involves an estimated 500 individuals or more, the Secretary of HHS must be notified as well. Notice must be given no more than 60 days after the breach is discovered, unless more time is needed for law enforcement purposes. The notification must include a description of the breach, the type of data involved, steps individuals should take to protect themselves, along with what is being done to investigate, mitigate, and guard against further harm, and whom to contact. However, if the data breached is deemed "secured" as defined by HHS, then notification is not necessary. This shows the importance of encryption, for if encrypted data is stolen, it is likely notification is not necessary.

Law enforcement may also need to be notified. Whom you should notify depends on the situation. If it is a hack, you may want to contact the Secret Service or the FBI. Law enforcement may instruct you to delay notification to consumers: Make sure you document all conversations, instructions, and steps followed.[8] Knowing who to call in what type of situation will help calm the chaos that ensues in a data breach.

Be prepared

Encryption should be used on all devices that contain PHI. Encryption is a process that obscures data so that it is unreadable to those who do not have the key to decipher it. It prevents access to PHI from lost or stolen devices. Any laptop with PHI that is not encrypted will raise red flags to regulators.

Any encryption is only as good as the password protecting it. You want a password that is both hard to crack and easy to remember. One suggestion is to make up a sentence that is easy to remember, then take the first letter of each word and include punctuation. For example, "I have two kids: Jack and Jill" can become the password Ih2k:JaJ.[9]

A written security plan should be in place, and staff should be informed of and trained on these procedures. Keep in mind that this is not an exhaustive list. The HIPAA Security rule lists numerous administrative, physical, and technical safeguards that should be instituted.[10] However, this list provides the most basic and bang-for-your-buck protection.

Be insured

Maintain full business and personal coverage. Coverage for data breaches exists. If a personal device contains business data, then both business and personal coverage are needed. For physicians who review patient information on personal devices, for example, a stolen laptop or hard drive would require both types of coverage. If you become aware of a breach, sit down and list the items taken and the information possibly compromised. Promptly notify your carriers.

Physicians with private offices cannot rely upon the property manager or the property owner for appropriate response to theft or breaches of PHI. Carefully review leases for provisions that require tenant notification of criminal activity on the premises. The lease-holder has no duty under HIPAA. Covered entities should only lease premises that guarantee appropriate response to theft.

Appropriate coverage, and knowledge, may not make you a dragon-slayer, but they will help you avoid being devastated by modern day cyber monsters. Responsible physicians will keep the foregoing points in mind while navigating these waters. ■

Note: This article does not constitute a legal opinion nor is it a substitute for legal advice. Legal inquiries about topics covered in this article should be directed to your attorney.

About the Authors

Nicole Li obtained her JD and Master of Bioethics from the University of Pennsylvania. She is the principal attorney at The Li Law Firm, which represents providers before the Department of Health and other entities. She effectively defends against adverse licensure action and post-payment audit demands and assists with establishing and maintaining credentials with payers. She may be reached through *www.lilawseattle.com*.

Matthew McCoy studies privacy and data security law at the University of Washington, where he earned degrees and certifications in English, Mathematics, and Information Security.

RESOURCES

HIPAA Security Rule: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/*

Summary: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html*

7. *http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf*. For help in determining whether you are covered, use the decision tool at: *http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp*.
8. Experian, Best Practices for a Healthcare Data Breach: What You Don't Know Will Cost You.
9. For more information, see *https://www.cs.cmu.edu/~help/security/choosing_passwords.html*.
10. 69 (online at *http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf*).